CLAIMS

1. A system for analyzing network traffic to use in performing network and security assessments by listening on a subject network, interpreting events, and taking action, comprising:

a policy specification file;

a network monitor processor for processing network packet data collected from said subject network; and

a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data.

2. The system of Claim 1, said policy monitoring component further comprising:

a parser for parsing said policy specification file;

a policy engine for synthesizing said parsed policy specification file and said processed network packet data, and for performing said assign dispositions and level of severity to said network events contained in said network packet data; and

a logger for logging and storing into an events database said synthesized information by said policy engine according to a logging policy file.

3. The system of Claim 2, further comprising:

a query mechanism for mining said stored data in said events database.

4. The system of Claim 2, further comprising:

an alarm script component for generating alarms based on said level of severity of said network events.

5. The system of Claim 2, further comprising means for said policy engine:

interpreting each protocol event; and

consulting said policy specification file as each protocol event is interpreted to ensure that an earliest determination of said disposition is reached.

6. The system of Claim 1, wherein said collected network packet data is captured in a file or is streams-based.

7. The system of Claim 1, further comprising:

a secure Web server comprising a Web server component and a report database for displaying reports online, said reports generated by said events database using a report script.

8. The system of Claim 1, further comprising:

a parser for generating an English description policy representation from said policy specification file.

9. The system of Claim 1, wherein said network monitor processor is used in standalone mode.

10. The system of Claim 1, wherein said network monitor processor and said policy monitoring component run on a same machine.

11. The system of Claim 1, further comprising:

a policy generator for generating said policy specification file.

12. The system of Claim 1, wherein said received network packet data is encoded.

13. A method for analyzing network traffic to use in performing network and security assessments by listening on a subject network, interpreting events, and taking action, said method comprising:

providing a policy specification file;

providing a network monitor processor for processing network packet data collected from said subject network; and

providing a policy monitoring component for receiving and processing said policy specification file, and receiving and processing said processed network packet data to assign dispositions to network events contained in said network packet data.

14. The method of Claim 13, said provided policy monitoring component further comprising:

providing a parser for parsing said policy specification file;

providing a policy engine for synthesizing said parsed policy specification file and said processed network packet data, and for performing said assign dispositions and level of severity to said network events contained in said network packet data; and

providing a logger for logging and storing into an events database said synthesized information by said policy engine according to a logging policy file.

15. The method of Claim 14, further comprising:

providing a query mechanism for mining said stored data in said events database.

16. The method of Claim 14, further comprising:

providing an alarm script component for generating alarms based on said level of severity of said network events.

17. The method of Claim 14, further comprising said policy engine:

interpreting each protocol event; and

consulting said policy specification file as each protocol event is interpreted to ensure that an earliest determination of said disposition is reached.

18. The method of Claim 13, wherein said collected network packet data is captured in a file or is streams-based.

19. The method of Claim 13, further comprising:

providing a secure Web server comprising a Web server component and a report database for displaying reports online, said reports generated by said events database using a report script.

20. The method of Claim 13, further comprising:

providing a parser for generating an English description policy representation from said policy specification file.

21. The method of Claim 13, wherein said network monitor processor is used in standalone mode.

22. The method of Claim 13, wherein said network monitor processor and said policy monitoring component run on a same machine.

23. The method of Claim 13, further comprising:

providing a policy generator for generating said policy specification file.

24. The method of Claim 13, wherein said received network packet data is encoded.

25. A method for interatively developing network security policy for a network, comprising:

creating an initial network security policy file;

ensuring said initial network security policy file is uploaded to a machine on said network;

running a network monitor on said network machine to collect said network traffic;

said network monitor outputting said collected network traffic in an output file, and passing said output file to a policy monitor;

said policy monitor analyzing said collected network traffic;

storing said analyzed network traffic in a database;

examining said analyzed network traffic in said database by querying said database using a query tool; and

modifying said initial network security policy file as needed until a comprehensive and desired policy file is attained.

26. The method of Claim 25, wherein said network machine is remote, and further comprising uploading said modified network security policy file to said remote network machine as needed.

27. The method of Claim 25, further comprising:

monitoring network traffic by using said attained comprehensive and desired policy file.

28. The method of Claim 27, wherein monitoring network traffic is on a continuous basis.

29. The method of Claim 25, further comprising:

generating reports from said database, and using said generated reports as input for further policy refinement and/or using said generated reports for continuously monitoring network traffic.

30. The method of Claim 29, further comprising:

encrypting said reports, and sending said encrypted reports to a remote secure Web server.

31. The method of Claim 30, further comprising:

accessing said reports on said remote server in a user-friendly manner.

32. The method of Claim 25, wherein creating an initial network security policy file, and modifying said network security policy file as needed use a policy generator tool.

33. A system for interatively developing network security policy for a network, said system comprising:

means for creating an initial network security policy file;

means for ensuring said initial network security policy file is uploaded to a machine on said network;

means for running a network monitor on said machine to collect said network traffic;

means for said network monitor outputting said collected network traffic in an output file, and passing said output file to a policy monitor;

means for said policy monitor analyzing said collected network traffic;

means for storing said analyzed network traffic in a database;

means for examining said analyzed network traffic in said database by querying said database using a query tool; and

means for modifying said initial network security policy file as needed until a comprehensive and desired policy file is attained.

34. The system of Claim 33, wherein said network machine is remote, and further comprising means for uploading said modified network security policy file to said remote network machine as needed.

35. The system of Claim 33, further comprising:

means for monitoring network traffic by using said attained comprehensive and desired policy file.

36. The system of Claim 35, wherein monitoring network traffic is on a continuous basis.

37. The system of Claim 33, further comprising:

means for generating reports from said database, and using said generated reports as input for further policy refinement and/or using said generated reports for continuously monitoring network traffic.

38. The system of Claim 37, further comprising:

means for encrypting said reports, and sending said encrypted reports to a remote secure Web server.

39. The system of Claim 38, further comprising:

means for accessing said reports on said remote server in a user-friendly manner.

40. The system of Claim 33, wherein means for creating an initial network security policy file, and modifying said network security policy file as needed uses a policy generator tool.

5